Sabotage-proof and censorship-resistant personal electronic health file

Patent Number: US2002194024
Publication date: 2002-12-19
Inventor(s): KLEINSCHMIDT PETER (DE)
Applicant(s):
Requested Patent: DE10126138
Application Number: US20020154828 20020528
Priority Number(s): DE20011026138 20010529
IPC Classification: G06F17/60
EC Classification:
Equivalents: EP1262855, A3, JP2003091456

Abstract

A protected electronic health file for managing all the health-relevant data, including earlier diagnoses and treatments, of a patient in the form of data capsules on a number of decentralized servers of a network with an access code which can be released by the patient wherein, with every change or addition to a called-up data capsule, the old data capsules in the network are erased and a new access code is formed, under which the changed data capsule is re-stored again in the network

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 26 138 A 1**

(51) Int. Cl.[7]: G 06 F 12/14

(21) Aktenzeichen: 101 26 138.1
(22) Anmeldetag: 29. 5. 2001
(43) Offenlegungstag: 12. 12. 2002

DE 101 26 138 A1

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Kleinschmidt, Peter, 91058 Erlangen, DE

(56) Entgegenhaltungen:
EP 10 99 996 A1
WO 01 18 631 A1

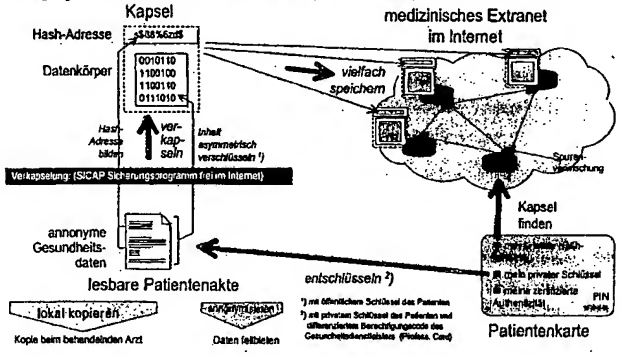
Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Sabotagesichere und zensurresistente persönliche elektronische Gesundheitsakte

(57) Gesicherte elektronische Gesundheitsakte zur Verwaltung aller gesundheitsrelevanten Daten, einschließlich früherer Diagnosen und Behandlungen, eines Patienten in mehreren dezentralen Servern mit dem Patienten freigebbaren Zugangsberechtigungen für Dritte, wobei die Daten ohne jegliche Identifizierungsdaten bezüglich der zugeordneten Person indexlos in einem Speichersystem mit vernetzten Servern, vorzugsweise verteilt, abgelegt sind, das keinen Bezug der Daten zum Patienten herstellt und wobei die Daten nur über Vorrichtungen oder Programme auffindbar und ablegbar sind, die jegliche Zugriffsspuren löschen.

Sabotagesichere und zensurresistente persönliche Gesundheitsakte (macht den Patienten zum Eigentümer der ihm zugänglichen Daten. Dezentrale, indexfreie Kapsel im Internet)



DE 101 26 138 A1

Beschreibung

[0001] Die Erfindung bezieht sich auf eine gesicherte elektronische Gesundheitsakte zur Verwaltung aller gesundheitsrelevanten Daten, einschließlich frühere Diagnosen und Behandlungen, eines Patienten in mehreren dezentralen Servern mit vom Patientenenten freigebbaren Zugangsberechtigungen für Dritte.

[0002] Für die aktuelle Behandlung eines Patienten ist es für den Behandelnden extrem wichtig, auf möglichst vollständige Daten über die Krankenvorgeschichte und patientenspezifische Daten, wie Impfungen, Allergien, Unverträglichkeiten usw. zugreifen zu können. Vollständigkeit bedeutet dabei nicht unbedingt hohe Detaillierung, siehe später. Andererseits sind diese Daten sensibel und dürfen nicht in falsche Hände gelangen. Neben seinem Gedächtnis verwendet der behandelnde Arzt Aufzeichnungen in Form einer Patientenakte und schreibt bei der Überweisung an einen anderen Arzt die wichtigsten Daten in ein Überweisungsschreiben. In der Praxis wird daraus ein Problem, wenn der Patient unvorhergesehen an einen neuen Arzt gerät, der aus Zeit- oder anderen Gründen keine Möglichkeit hat, an die Daten seiner Kollegen zu gelangen. Im Übrigen stehen diese Daten dem Patienten nur beschränkt zur Verfügung, was künftig zum technischen und juristischen Problem werden könnte, wenn dem Patienten verschiedene Gesundheitsdienste im Netz angeboten werden.

[0003] Bisher gibt es bereits zahlreiche Vorschläge und Testinstallationen, die mittels elektronischer Kommunikationsmittel dieses Problem zu lösen versuchen. Sie basieren zum einen auf einer persönlich bei sich zu tragenden Patientenakte, zum Beispiel in Form einer elektronischen Chipkarte oder zum anderen auf einem zentralen Netzserver, auf den jeder Arzt zugreifen können soll. Die reine Kartenlösung, die bereits seit Jahren diskutiert wird und in einigen Ländern eingeführt ist, hat dabei die Problematik, dass zum einen die Datenmenge nur begrenzt ist, dass keine Verfügbarkeit der Daten für Teledienste gegeben ist, dass sie nur mechanisch in mobile Computing integrierbar ist und dass keine Eingabemöglichkeit durch Tastatur, durch Barcodes oder elektronische Tags zur Verfügung steht.

[0004] Die vorstehend angesprochene zentrale Patientenakte wird von Netzbefürwortern immer wieder propagiert. Dabei ergibt sich zum einen die Schwierigkeit, dass ohne einheitliche Daten-Normen eine solche Patientenakte praktisch undurchführbar ist. Darüber hinaus ergeben sich aber auch juristische Probleme zur Datenverwendung, aufwändige Maßnahmen für eine letztlich doch nicht garantierbare Sicherheit und dadurch die Gefahr eines Verlustes der Daten durch Sabotage sowie des Missbrauchs der Daten. Auch eine bereits probeweise eingeführte Einstellung privater Akten bei Providern im Internet kann das angesprochene Problem nicht lösen, da sowohl eine unkontrollierbare Datenweitergabe zu befürchten ist, die Privatheit der Daten nicht garantiert ist und die Daten auch in vielen Fällen untereinander inkompatibel sind.

[0005] Der Erfindung liegt daher die Aufgabe zugrunde, eine gesicherte elektronische Gesundheitsakte zu schaffen, die sabotagesicher und zensurresistent ist und eine erhöhte Sicherheit gegen unbefugte Weitergabe oder unbefugte Benutzung der Daten beinhaltet.

[0006] Zur Lösung dieser Aufgabe ist erfindungsgemäß vorgesehen, dass die Daten ohne jegliche Identifizierungsdaten bezüglich der zugeordneten Person indexlos in einem Speichersystem mit vernetzten Servern abgelegt sind, das keinen Bezug der Daten zum Patienten herstellt und dass die Daten nur über Vorrichtungen oder Programme auffindbar und ablegbar sind, die jegliche Zugriffsspuren löschen.

[0007] Die Daten sollen dabei bevorzugt in Form von hier sogenannten Datenkapseln mit gegebenenfalls unterschiedlichen Zugriffcodes im Speichernetzwerk gespeichert sein, wobei dieses Speichernetzwerk ein überall verfügbares Netzwerk nach Art des Internet sein soll, in dem gegebenenfalls ein zensurresistentes Extranetz wie das sogenannten "freenet" zur Speicherung der Daten ausgebildet sein kann. Dieses "freenet" kann im Internet durch eine zertifizierte Software jedem zur Verfügung gestellt werden, wobei diese zertifizierte Software garantiert, dass sie außer den beschriebenen Funktionen keine Hintertüren besitzt, die den illegalen Zugriff zu den Daten ermöglichen könnte.

[0008] Das angesprochene Extranetz im Internet kann dabei so ausgebildet sein, dass die Daten-Kapseln selbstorganisiert an unterschiedliche Server weitervermittelt und mehrfach identisch abgespeichert werden, sodass sich dabei möglicherweise auftretende Spuren verlieren und nicht zurückverfolgbar sind. Darüber hinaus hat diese mehrfache Abspeicherung – wobei der Patient durch Parameterisierung eines Zählers die Zahl der identischen Sicherheitskopien bestimmen kann – den Vorteil, dass der zufällige Absturz eines Speichers, der eine der anonymisierten Daten-Kapseln der elektronischen Gesundheitsakte enthält, nicht zu einem Verlust dieser Daten führt, da ja die Mehrzahl der Sicherungskopien – selbst nach mehrfacher Verteilung im Speichernetz – nicht auf dem gleichen Server abgelegt sein kann.

[0009] Unabhängig davon, dass eine solche Daten-Kapsel ja sowieso nur mithilfe des beliebig kompliziert aufbaubaren Zugangscodes gelesen werden kann, den nur der Patient hat und den er dritten, wie Ärzten, Dienstleistern, Krankenkassen oder dergleichen nur in Ausnahmefällen und darüber hinaus möglicherweise auch nur im beschränkten Umfang zur Verfügung stellt, kann zur zusätzlichen Absicherung noch vorgesehen sein, dass die Daten verschlüsselt gespeichert sind, wobei zur Verschlüsselung einer Kapsel bevorzugt ein asymmetrischer Schlüssel verwendet wird mit einem öffentlichen Schlüssel des Patienten zum Verschlüsseln der Patientenakte und einem privaten Schlüssel des Patienten zum Entschlüsseln, wobei der private Schlüssel oder das Schlüsselpaar weiterer Bestandteil der persönlichen Berechtigungsinformation, also des persönlichen Zugriffscodes für das Lesen des Inhalts einer Datenkapsel darstellen.

[0010] Die Zugriffscodes können in weiterer Ausgestaltung der Erfindung eine Hash-Adresse umfassen, die aus einem, aus definierten Bestandteilen der Patientendaten bebildeten Hash-Code und einem weiteren Zeichen zur Erzeugung einer eindeutigen Adresse gebildet ist. Statt eines solchen ergänzten Hash-Algorithmusses können selbstverständlich aber auch andere gleichwertige Verfahren zur Bildung einer unverwechselbaren Adresse verwendet werden. Diese Adresse kann so lange wie gewünscht beibehalten werden, auch bei Veränderung des Inhalts der Gesundheitsakte.

[0011] Gemäß einem weiteren Merkmal der vorliegenden Erfindung kann vorgesehen sein, dass die Inhalte der Datenkapseln durch spezielle Unter-Zugriffscodes von entsprechend autorisierten Dritten, zum Beispiel Ärzten, Dienstleistern, Pharmafirmen, Krankenkassen oder dergleichen in begrenztem Umfang lesbar sind, wobei hierfür bevorzugt Zugangseinrichtungen vorgesehen sind, die es ermöglichen, bestimmte Teile der Daten als Statistikdaten zu extrahieren, zu ergänzen, zu kombinieren und zu schematisieren.

[0012] Die anonymisierten Statistikdaten sollen dabei zur weiteren Verwendung, insbesondere für den Abruf durch Pharmafirmen oder Krankenkassen, die hierfür dem autorisierenden Patienten gewisse Vorteile oder Vergütungen zukommen lassen, in – auf Veranlassung des Patienten – spezielle Statistik-Kapseln eingegeben und gespeichert werden,

die mit einer global geltenden Kapseladresse versehen sind. Es bedarf also keiner Freigabe des eigentlichen Zugriffscodes zu allen Daten der persönlichen Gesundheitsakte des Patienten um diese Statistikfunktionen mit erfüllen zu können.

[0013] Der oder die Zugriffscodes können dabei gemäß einem weiteren Merkmal der vorliegenden Erfindung in spezielle, vorzugsweise tragbare Zugangsgeräte, implementiert sein, wie beispielsweise eine Chipkarte, ein Handy, eine Uhr, ein Amulett oder dergleichen, sie können aber auch in einen öffentlichen Zugangsgegenstand, also beispielsweise ein Netzportal oder dergleichen eingegeben werden. Das Zugangsgerät kann dabei in an sich bekannter Weise durch ein Authentifizierungssystem gesichert sein, wie beispielsweise durch eine PIN-Nummer, um bei Verlust des Zugangsgerätes einem Missbrauch vorzubeugen.

[0014] Um einen vollständigen Datenverlust im Falle eines Verlustes einer Kapseladresse zu vermeiden, kann in weiterer Ausgestaltung der Erfindung auch vorgesehen sein, dass zumindest Teile der Patientenakten in Ablagevorrichtungen bei den Ärzten, Dienstleitern oder dergleichen, gegebenenfalls auch nur teilweise für diese lesbar, gespeichert sind, die für den Patienten zugänglich sind, um im Falle des Verlustes einer Kapseladresse eine Rekonstruktion einer neuen Daten-Kapsel aus diesen Kopien zu ermöglichen.

[0015] Die wichtigen Gesundheitsinformationen, die in einer erfindungsgemäßen sabotagegesicherten und zensurresistenten persönlichen elektronischen Gesundheitsakte sicher und doch für vielfältige Gesundheitsanwendungen abrufbar gespeichert sein sollen, umfassen zum einen langfristige, im Interesse des Patienten geheimzuhaltenden Informationen, also alle jene historischen bis aktuellen Daten sowie Spekulationen und Ratschläge, die für eine jedwede zukünftige Beratung oder Behandlung als bedeutungsvoll erachtet werden. Dazu gehören Anamnese, Befunde, Abschlussberichte sowie Belege Medizinischer Stadien, wie Fotos, diagnostische Bilder, Videos und Tondokumente. Hypothesen, Zwischenschritte, Irrwege, negative Befunde und so weiter sind nur in ihrem Ergebnis und gemäß ihrer voraussichtlichen zukünftigen Bedeutungen, nicht aber in allen Einzelheiten zu vermerken. Dabei kann ein Teil dieser Daten direkt auf dem persönlichen Zugangsgerät zusätzlich zu den persönlichen Berechtigungsinformationen lokalisiert sein (z. B. Notfalldaten) und/oder als Zeiger, das heißt als spezielle Adresse, ausgebildet sein, über den man ohne Barrieren direkt über das überall verfügbare Netzwerk mithilfe dessen die erfindungsgemäße Gesundheitsakte realisiert wird – zum derzeitigen Zeitpunkt wäre dies speziell das sogenannte Internet – an diese Daten gelangt.

[0016] Zum anderen handelt es sich um kurzfristige vertrauliche Daten, wie Behandlungsdaten, Verschreibungen, Messwerte, Beobachtungen, Ratschläge usw., die nach einiger Zeit ausgewertet oder erledigt sind und gelöscht werden. Die daraus resultierenden Daten werden in angemessenen Abständen zum Bestand der langfristigen Daten hinzugefügt. Für kurzfristige und langfristige Daten können dabei – wie es bereits weiter oben vorgeschlagen worden ist – unterschiedliche Kapseln mit unterschiedlichen Hash-Adressen verwendet werden, wobei beide Hash-Adressen mithilfe ein und desselben individuellen Zugangsgeräts oder auch mit unterschiedlichen, voneinander getrennten Zugangsgeräten erreicht werden können. Die Auswahl erfolgt im ersteren Fall mittels Bediensoftware oder mittels einer Konfigurationsmöglichkeit auf dem individuellen Zugangsgerät.

[0017] Zusammenfassend ist also festzuhalten, dass die erfindungsgemäße elektronische Gesundheitsakte durch Datenstrukturen gekennzeichnet ist, sodass die Daten nur in dem Umfang gelesen werden können, wie der Nutzer Rechte dazu dem Patienten gegenüber ausweisen kann. Der Patient kann selbst auch alle Teile der Akten lesen, sofern er auf einen psychologischen Schutz vor schockierenden Daten verzichtet und hat auch Bereiche in denen er schreiben, also Daten verändern, kann. Die bekannte Professional-Card erlaubt den Ärzten ebenfalls nur Zugriffe auf bestimmte Teile. Aufgrund doppelter (mehrfacher) Verschlüsselung bleiben ihm aber Teile unlesbar (sogenanntes Rollenkonzept). Der Patient kann auch mehrere Kapseln definieren und entscheiden, zu welchen er wem Zugang gewährt. Das Rollenkonzept kann über Schlüssel oder andere Zugriffsbeschränkungen realisiert werden.

[0018] Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus der weiteren Beschreibung einiger Ausführungsbeispiele sowie anhand der Zeichnung. Dabei zeigen:

[0019] **Fig.** 1 Eine schematische Darstellung der Organisation einer erfindungsgemäßen gesicherten persönlichen Gesundheitsakte im Internet,

[0020] **Fig.** 2 eine Darstellung der persönlichen Gesundheitsakte für die private Bearbeitung durch den Patienten,

[0021] **Fig.** 3 eine der **Fig.** 2 entsprechende Darstellung der Bearbeitungsmöglichkeiten der persönlichen Gesundheitsakte durch den Arzt,

[0022] **Fig.** 4 eine Darstellung der Dokumententypen der Gesundheitsakte mit einem Beispiel für die Aufteilung der Informationen auf verschiedene Kapseln mit unterschiedlichen Hash-Adressen,

[0023] **Fig.** 5 den Ablauf einer Behandlung, Überweisung und Rezeptstellung mit Karte und Patientenakte im Internet unter Verwendung einer erfindungsgemäßen gesicherten Gesundheitsakte und

[0024] **Fig.** 6 Aufbau und Organisation einer persönlichen Zugangskarte zur internetpassierten erfindungsgemäßen Gesundheitsakte.

[0025] Die **Fig.** 1 zeigt schematisch den Aufbau einer sabotagesicheren und zensurresistenten persönlichen Gesundheitsakte, die den Patienten zum Eigentümer der ihm zugänglichen Daten macht, wobei die Gesundheitsakte eine oder mehrere dezentrale indexfreie Kapseln im Internet umfasst. In den **Fig.** 2 und 3 sind die verschiedenen Möglichkeiten des Einspeicherns und Auslesens in oder aus der im Internet gespeicherten Gesundheitsakte einmal für den Patienten selbst und einmal als Ausführungsbeispiel eines zugelassenen Nutzers durch den Arzt dargestellt, wobei die Authentifizierung und die Hash-Adresse, die grundsätzlich auf verschiedenartigen Zugangsgeräten angeordnet sein kann, wie beispielsweise einem Handy, einer Uhr, einem Amulett, einem elektronischen Etikett in Form eines Transponders, einem Barcodeleser oder durch Codeeingabe per Tastatur, wie im gezeigten Ausführungsbeispiel anhand einer Chipcard realisiert ist, die in ihrem Aufbau und in ihrer Datenorganisation und noch etwas genauer dargestellt ist. So kann die persönliche Gesundheitsakte vom Arzt gemäß **Fig.** 3 wie folgt verwendet werden:

Der Patient, körperlich anwesend, überlässt dem Arzt physikalische persönliche Patientenkarte, Arzt findet Kapsel(n) im Internet und öffnet sie mit Patientenkarte (und Arztkarte). Er trägt Behandlungstatsache und Behandlungstermin ein, macht eine lokale Kopie und verkapselt neu mit (zum Beispiel ihm bekannter oder unbekannter) neuer letzter Hash-Adresse und setzt die neue Kapsel wieder ins Internet ab. Wenn sich dabei die Hash-Adresse geändert hat, werden alle alten Kapseln durch Ausführung entsprechend vorzusehender Programmteile gelöscht. Der Arzt arbeitet ab jetzt bis zu einem wichtigen Zwischenabschluss auf seiner lokalen Kopie und verwendet diese für Überweisungen und Teledienste. Der Patient kann sich mittels Authentifikation im Netz ausweisen. Der Nachtrag der Behandlungsergeb-

nisse auf der Patientenkarte muss separat erfolgen. Bei asymmetrischem Schlüssel auch ohne Patientenkarte möglich, solange ihm gültige Hash-Adresse benannt und nicht verändert wird.

[0026] In **Fig.** 4 sind die verschiedenen Dokumententypen der Gesundheitsakte nach Art ihrer Ermittlung und ihrer Bedeutung für die Gesundheitsakte und auch im Hinblick auf die unterschiedlich hohen Verschlüsselungs- und unterschiedlichen Zugangsmöglichkeiten angedeutet. Speziell die in der sogenannten Kapsel B gespeicherten Patientendaten – auch hier könnte es sich selbstverständlich wieder um mehrere unterschiedliche Datenkapseln handeln – betreffen Daten, die weniger geheimhaltungsbedürftig sind und zu denen beispielsweise auch sogenannte Statistikdaten gehören, die von entsprechenden Dienstleistern (gegen entsprechende Vergütung an den Patienten) jederzeit abrufbar sind.

[0027] Der Weg bei einer Behandlung, Überweisung oder Rezeptstellung mithilfe von Chipkarten als Zugangskarten zur elektronischen persönlichen Gesundheitsakte im Internet sind in **Fig.** 5 schematisch als Diagramm angedeutet, während – wie bereits angesprochen – die **Fig.** 6 eine Chipkarte als persönliche Zugangskarte des Patienten zu seiner elektronisch gespeicherten Gesundheitsakte anhand der grafisch angedeuteten verschiedenen Zugriffsmöglichkeiten näher erläutert.

[0028] Um die persönliche Gesundheitsakte für Telemedizin zu verwenden, arbeitet der Arzt zum Beispiel mit den Daten aus seiner lokalen Kopie und mit der von ihm bevorzugten Technik und verwendet diese für die Teledienste. Der Patient kann sich mittels seiner Authentifikation im Netz ausweisen und somit mit Berechtigung an Telediensten teilnehmen.

[0029] Die persönliche Patientenakte kann weitere Bereiche besitzen, in die Daten geschrieben werden können und aus denen Daten gelesen werden können, wobei diese Bereiche für die Hash-Bildung ausgespart werden, sodass Dateneintragungen in diese Bereiche zu keiner Veränderung der Hash-Adresse führen. Diese Bereiche können auch für privates Gesundheitsmanagement verwendet werden, sodass hier Messwerte aus Geräten und Daten von Labels von Medikamenten und Heil- und Hilfsmitteln eingetragen werden.

Patentansprüche

1. Gesicherte elektronische Gesundheitsakte zur Verwaltung aller gesundheitsrelevanten Daten, einschließlich früherer Diagnosen und Behandlungen, eines Patienten im mehreren dezentralen Servern mit vom Patienten freigebbaren Zugangsberechtigungen für Dritte, **dadurch gekennzeichnet**, dass die Daten ohne jegliche Identifizierungsdaten bezüglich der zugeordneten Person indexlos in einem Speichersystem mit vernetzten Servern, vorzugsweise verteilt, abgelegt sind, das keinen Bezug der Daten zum Patienten herstellt und dass die Daten nur über Vorrichtungen oder Programme auffindbar und ablegbar sind, die jegliche Zugriffsspuren löschen.
2. Gesundheitsakte nach Anspruch 1, dadurch gekennzeichnet, dass die Daten in Form von Datenpaketen (Daten-Kapseln) mit gegebenenfalls unterschiedlichen Zugriffscodes gespeichert sind.
3. Gesundheitsakte nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Daten in einem überall verfügbaren Netzwerk, insbesondere im Internet gespeichert sind.
4. Gesundheitsakte nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Daten ein einem zensurresistenten Extra-Netz ("freenet") gespeichert sind.
5. Gesundheitsakte nach Anspruch 4, dadurch gekennzeichnet, dass das Extra-Netz so ausgebildet ist, dass die Daten-Kapseln selbstorganisiert an unterschiedliche Server weitervermittelt und mehrfach identisch abgespeichert werden, sodass sich dabei möglicherweise auftretende Spuren verlieren und nicht zurückverfolgbar sind.
6. Gesundheitsakte nach Anspruch 5, dadurch gekennzeichnet, dass der Patient durch Parameterisierung eines Zählers die Zahl der identischen Sicherheitskopien bestimmen kann.
7. Gesundheitsakte nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass die Daten verschlüsselt abgespeichert sind.
8. Gesundheitsakte nach Anspruch 7, gekennzeichnet durch die Verwendung asymmetrischer Schlüssel.
9. Gesundheitsakte nach Anspruch 8, dadurch gekennzeichnet, dass der private Schlüssel oder das Schlüsselpaar ein Bestandteil der persönlichen Berechtigungsinformation für das Lesen des Inhalts auf dem persönlichen Teil einer gespeicherten Datenkapsel ist.
10. Gesundheitsakte nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die Zugriffscodes eine Hash-Adresse umfassen, die aus einem (aus definierten Bestandteilen der Patientendaten gebildeten) Hash-Code und weiteren Zeichen zur Erzeugung einer eindeutigen Adresse gebildet ist.
11. Gesundheitsakte nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass die Inhalte der Datenkapseln durch spezielle Unter-Zugriffscodes von entsprechend autorisierten Dritten, zum Beispiel Ärzten, Dienstleistern, Pharmafirmen oder dergleichen in begrenztem Umfang lesbar sind.
12. Gesundheitsakte nach Anspruch 11, dadurch gekennzeichnet, dass Zugangseinrichtungen vorgesehen sind, die es ermöglichen, bestimmte Teile der Daten als Statistik-Daten zu extrahieren, zu ergänzen, zu kombinieren und zu schematisieren.
13. Gesundheitsakte nach Anspruch 12, dadurch gekennzeichnet, dass die anonymisierten Statistikdaten in eine spezielle Statistik-Kapsel eingegeben und gespeichert werden, die mit einer global geltenden Kapsel-Adresse versehen ist.
14. Gesundheitsakte nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, dass die Zugriffscodes in speziellen, vorzugsweise tragbaren Zugangsgeräten (wie zum Beispiel Karte, Handy, Uhr, Amulett oder dergleichen) implementiert sind, die ihrerseits durch ein Authentifizierungssystem gesichert sind.
15. Gesundheitsakte nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass zumindest Teile der Patientenakten in Ablagevorrichtungen bei Ärzten, Dienstleistern oder dergleichen gespeichert sind, die für den Patienten zugänglich sind (und im Falle des Verlustes einer Kapsel-Adresse eine Rekonstruktion einer neuen Datenkapsel aus diesen Kopien ermöglichen).

Hierzu 6 Seite(n) Zeichnungen

Sabotagesichere und zensurresistente persönliche Gesundheitsakte (macht den Patienten zum Eigentümer der ihm zugänglichen Daten. Dezentrale, indexfreie Kapsel im Internet)

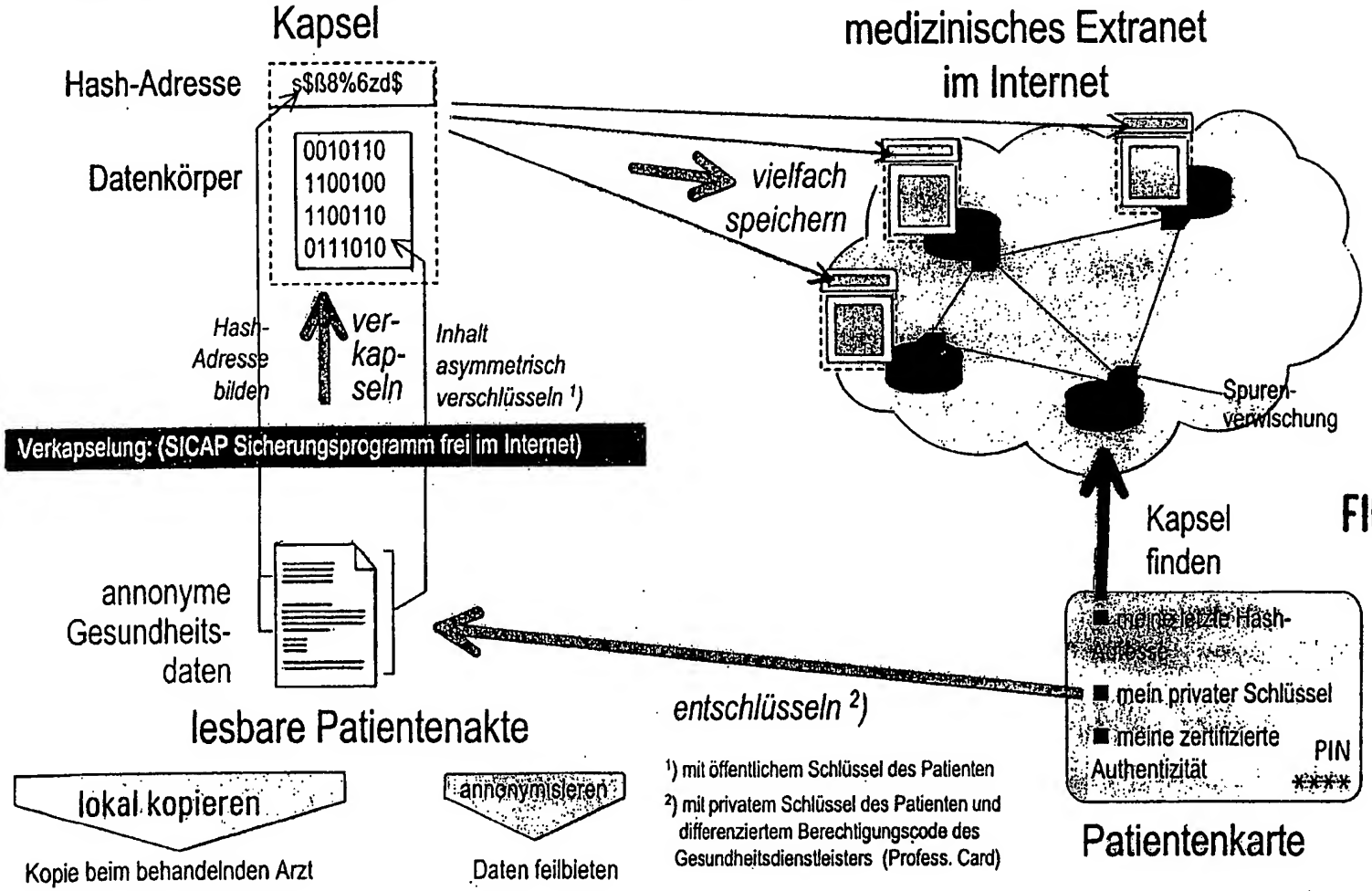


FIG 1

Nummer: DE 101 26 138 A1
Int. Cl.?: G 06 F 12/14
Offenlegungstag: 12. Dezember 2002

Nummer: DE 101 26 138 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 12. Dezember 2002

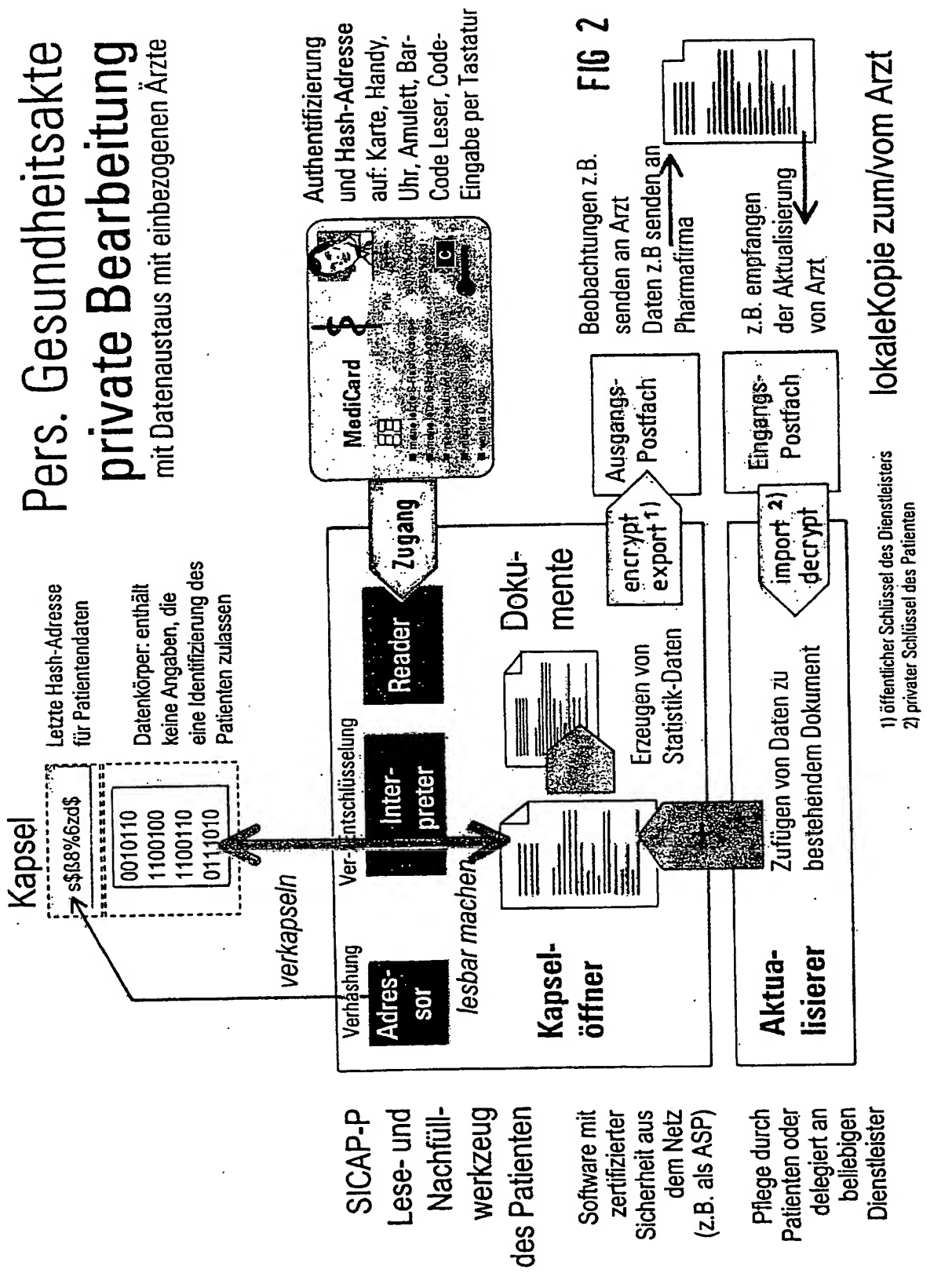


FIG 2

102 500/243

Nummer: DE 101 26 138 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 12. Dezember 2002

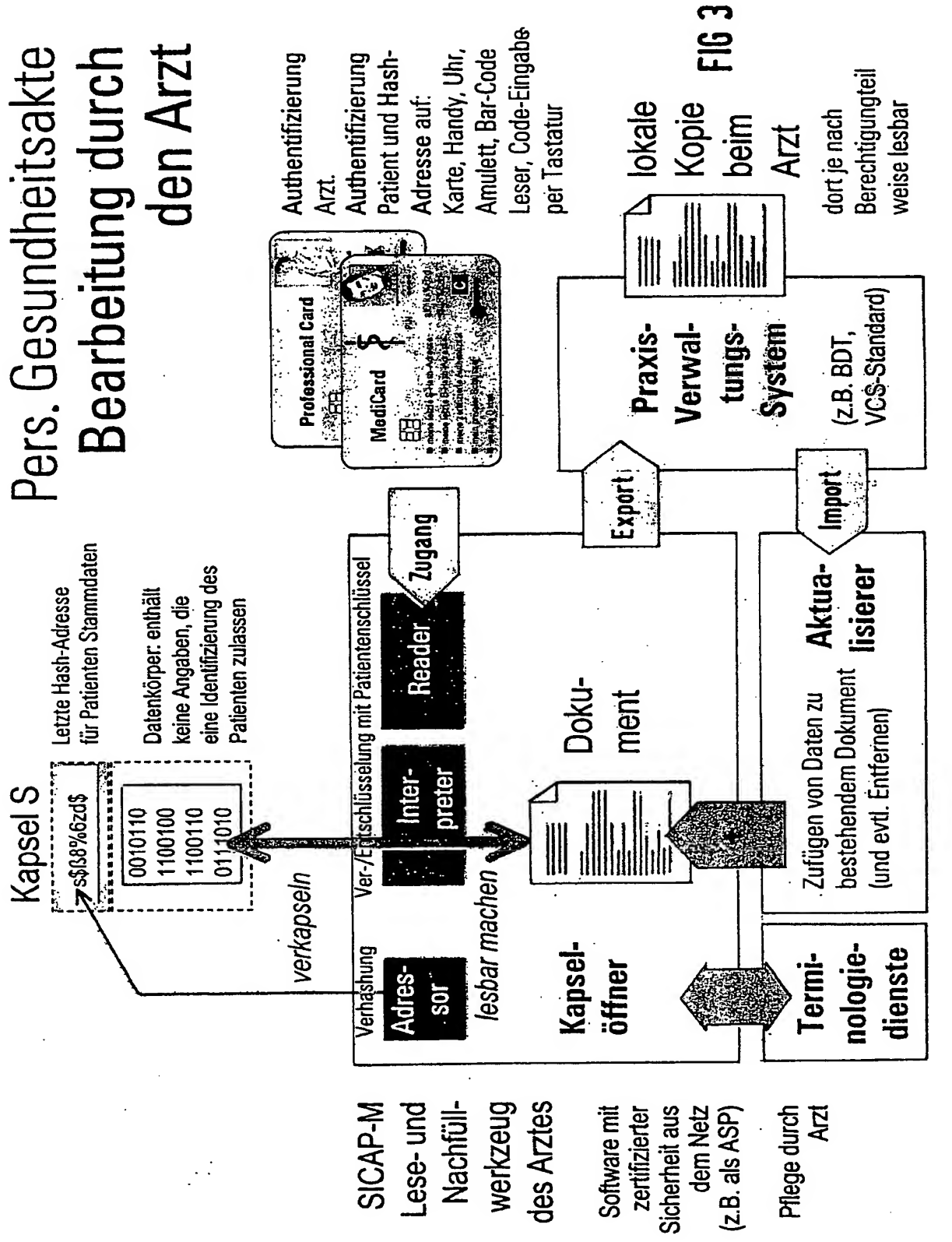


FIG 3

Dokumenttypen der Gesundheitsakte

❶ Von allen unverschlüsselt lesbare Daten (z.B. Notfalldaten)

❷ Langfristig gültige Dienstleistungsdaten, die von Dienstleistern ergänzt werden und die von diesen lesbar und schreibbar sind sowie vom betroffenen Indviduum (Eigentümer) nur lesbar sind. (z.B. Daten der Patientenakte wie: Anamnese, Impfungen, Unverträglichkeiten, Befunde, Bilder). Die Leserechte werden durch Rollen geregelt. Die Parametrisierung erfolgt über die Autentifizierungsmerkmale. Der Eigentümer kann alle Daten lesen außer solchen, bei denen der Eigentümer darauf verzichtet, ihren Inhalt zu kennen.

❸ Dynamische Dienstleistungsdaten, die von Dienstleistern an andere, im Vorraus nicht bekannte, z.B.durch den Patienten auszusuchende Dienstleister übermittelt werden und die von diesen lesbar und schreibbar sind sowie vom betroffenen Indviduum nur lesbar sind (z.B. Rezepte, Überweisungen, Diagnostiken an unbekannt).

❹ Dynamische Dienstleistungsdaten die vom Patienten einem oder mehreren, z.T. auch anfänglich unbekannten Dienstleistern zur Verfügung gestellt werden (z.B. Monitoringdaten, Fragen, ..).

❺ Vertretungsverfügungen: Vollmachten, Empfangsberechtigungen, ...

❻ Persönliche verschlüsselte Daten, die nur dem Eigentümer zugänglich sind (Tresor für beliebige, computerlesbarer Dokumente).

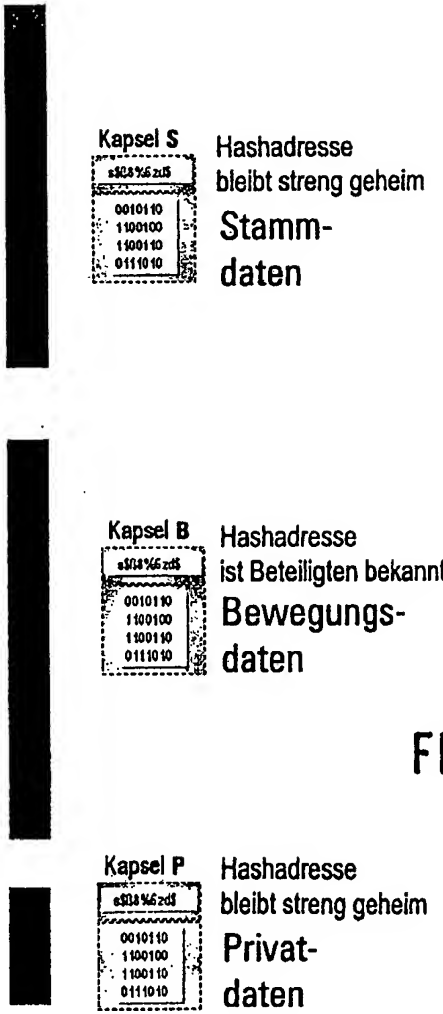


FIG 4

Nummer:
Int. Cl.7:
Offenlegungstag:

DE 101 26 138 A1
G 06 F 12/14
12. Dezember 2002

Nummer: DE 101 26 138 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 12. Dezember 2002

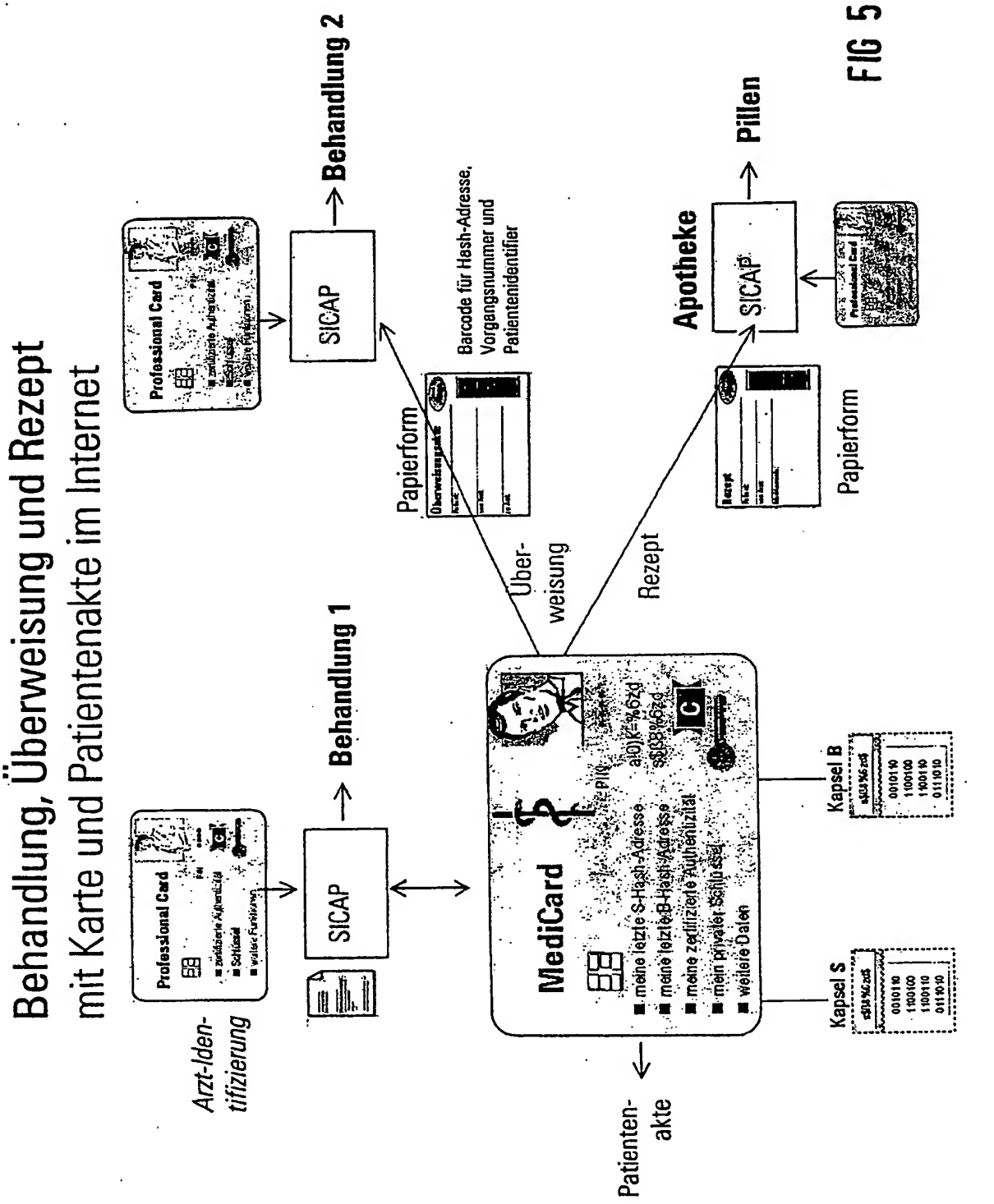


FIG 5

Nummer: DE 101 26 138 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 12. Dezember 2002

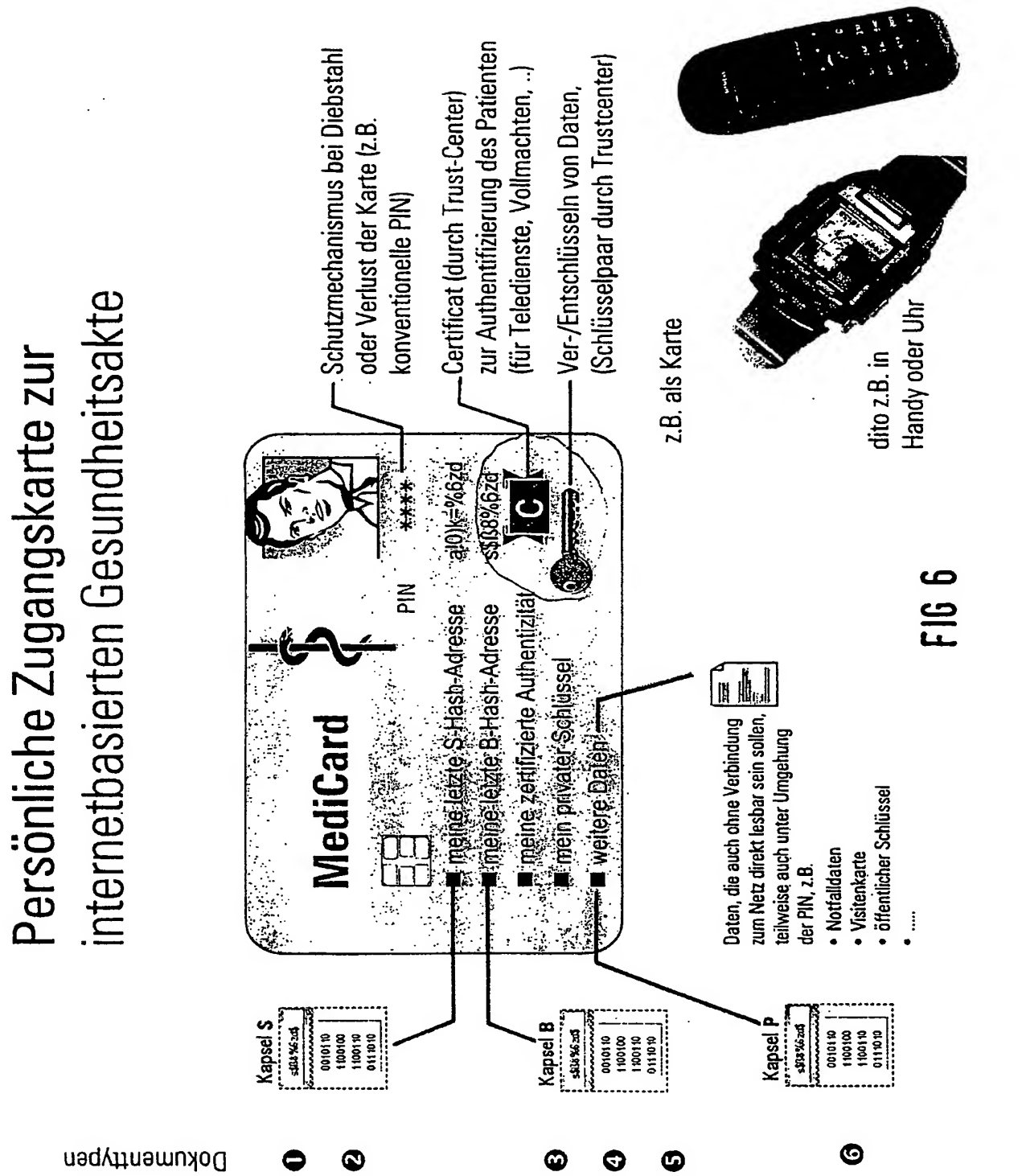


FIG 6